

December 10, 2021

TRANSMITTED VIA ELECTRONIC MAIL

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Mitchell N. Roth
Tysons Corner Office
(703) 485-3536 (direct)
mroth@rothjackson.com

RE: Comments of SipNav LLC Regarding Commission's Fifth Notice of Proposed Rulemaking in CG Docket No. 17-59 and Fourth Further Notice of Proposed Rulemaking in WC Docket. 17-97.

Dear Ms.Dortch:

This law firm represents SipNav LLC ("SipNav"). On behalf of SipNav, we submit these Comments regarding the Commission's Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 and Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97. This FNPRM imposes restrictions on gateway providers to combat illegal robocalls.

I. Introduction.

SipNav operates a hosted-switch platform. It is an all-in-one carrier solution for SIP network elements which operates on a private hosted infrastructure. SipNav's scalable solution allows it to offer its services to carrier customers that range from those that process only a few thousand concurrent calls to those process more than one hundred thousand concurrent calls. SipNav provides its carrier customers with a wealth of tools to combat the transmission of illegal robocalls.

The Commission's proposed rulemaking imposes significant obligations on gateway providers who have no involvement in the initiation of illegal robocalls. It imposes standards with associated expensive compliance obligations on the providers while ignoring the scammers that are initiating the calls at issue. This results in a never-ending game of whack-a-mole as scammers continuously utilize

RICHMOND

1519 Summit Avenue, Suite 102, Richmond, VA 23230
P: 804-441-8440 F: 804-441-8438

TYSONS CORNER

8200 Greensboro Drive, Suite 820, McLean, VA 22102
P: 703-485-3535 F: 703-485-3525

new carriers to enter the US telecommunications network once an existing route is closed by a gateway provider.

SipNav respectfully suggests that the Commission consider an alternate mechanism for curtailing scam robocalls – one that leverages the media IP address of the servers that actually initiate the known scam calls.

The media IP address of the call-initiating server is appended to all calls. When scam robocalls are identified, the call's media IP address can be extracted and circulated to switch providers. Switch providers can, in turn, block all subsequent calls with the identified media IP address from entering and passing through their switches. This can be done at the gateway provider's switch, thereby preventing the calls from entering the US telecommunications network.

Leveraging the media IP address appended to known scam calls has the added benefit of allowing law enforcement to identify the physical location of the data center that houses the server that initiated the calls. Once the data center is located, the owner of the server can be identified.

II. Discussion.

Robocalls are initiated by servers that are attached to a telecommunications network. The servers are assigned a unique media IP address by the data centers in which they reside. No two servers in the world have the same media IP address. The data centers assign the media IP address when the equipment is connected to the center's Internet trunks. The name and exact location of the assigning data center can be identified from the media IP address using publicly available resources. Media IP addresses cannot easily be changed by the operator of a particular piece of equipment.

All calls initiated by a particular server – both voice calls and robocalls – have the server's unique media IP address appended to it from the point of origination through the point of termination.



RICHMOND

1519 Summit Avenue, Suite 102, Richmond, VA 23230
P: 804-441-8440 F: 804-441-8438

TYSONS CORNER

8200 Greensboro Drive, Suite 820, McLean, VA 22102
P: 703-485-3535 F: 703-485-3525

When a particular call is identified as one that has transmitted a scam robocall, switch companies, such as SipNav, are able to identify the media IP address of the server that initiated the scam robocall and block all future calls that carry the same media IP address. Doing so blocks all future calls by the server that initiated the scam robocall.

Importantly, the switch provider's ability to block these calls is independent of the gateway provider.¹ This targeted and nuanced approach blocks only the calls initiated by the offending server while allowing all "clean" calls to pass through the switch.

Additionally, with the media IP address of the server that initiated an illegal robocall, law enforcement organizations can identify the data center that housed the server that initiated the illegal call who, in turn, can identify the owner/operator of the server in question (i.e., the call initiator).

SipNav maintains a blacklist of media IP addresses that have been linked to scam robocalls. SipNav provides its customers with the ability to run calls that seek to pass through its switch against this blacklist and block those calls that were originated from servers with the media IP address of those known scammers. By doing so, servers that initiated these calls will never be able to transmit calls through SipNav's hosted switch. Once other switch providers adopt similar practices, calls initiated by servers that transmit illegal robocalls will not be able to access the US telecommunications network.

To date, the Commission's detection and enforcement of robocall scammers has focused largely, if not exclusively, on the caller ID signal transmitted with illegal calls. Caller ID signals can easily be manipulated by scammers. SipNav invites the Commission to leverage the data transmitted on SIP calls

¹ Media IP addresses are invaluable to law enforcement agencies as well: These agencies can use both publicly and privately available resources to pinpoint the hosts of the servers that were used to transmit the illegal calls. Presumably, these hosts can then learn the identities of the scammers who initiated the calls.



RICHMOND

1519 Summit Avenue, Suite 102, Richmond, VA 23230
P: 804-441-8440 F: 804-441-8438

TYSONS CORNER

8200 Greensboro Drive, Suite 820, McLean, VA 22102
P: 703-485-3535 F: 703-485-3525

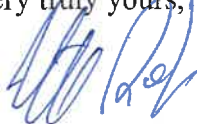
– especially the initiating servers’ media IP address -- to affirmatively block calls initiated by servers that have transmitted illegal robocalls and identify the location and owners of such servers for prosecution. This technique attacks the hardware used by, and exposes the identity of, those that seek to originate illegal robocalls into the United States. This contrasts with traditional enforcement mechanisms that: i) focuses on the transmitted caller ID signal which can be changed with every initiated call; and ii) places large burdens on the gateway providers that are not responsible for, and play no role in, the origination of the illegal robocalls.

III. Conclusion.

By leveraging the media IP address of known scam robocalls, carriers and their switch providers are able to permanently end the ability of the call-initiating servers to send calls into the United States. This nuanced approach focuses solely on the known bad actors and is more effective than relying on statistical analyses in identifying *probable* illegal robocalls.

Please contact me with any questions the Commission may have.

Very truly yours,



Mitchell N. Roth

MNR:mmi



RICHMOND

1519 Summit Avenue, Suite 102, Richmond, VA 23230
P: 804-441-8440 F: 804-441-8438

TYSONS CORNER

8200 Greensboro Drive, Suite 820, McLean, VA 22102
P: 703-485-3535 F: 703-485-3525